Journal of Computer and System Sciences 81 (2015) 1059–1087

Contents lists available at ScienceDirect

Journal of Computer and System Sciences

www.elsevier.com/locate/jcss

Normality in non-integer bases and polynomial time randomness

Javier Ignacio Almarza [a], Santiago Figueira [b,c,*]

[a] Departamento de Matemática, FCEyN, Universidad de Buenos Aires, Argentina
[b] Departamento de Computación, FCEyN, Universidad de Buenos Aires, Argentina
[c] CONICET, Argentina

ARTICLE INFO

Article history:
Received 31 October 2014
Received in revised form 13 April 2015
Accepted 16 April 2015
Available online 29 April 2015

Keywords:
Algorithmic randomness
Polynomial time randomness
Normality
Subshift
Pisot number
Deterministic finite automaton
Martingale

ABSTRACT

It is known that if $x \in [0, 1]$ is polynomial time random then x is normal in any integer base greater than one. We show that if x is polynomial time random and $\beta > 1$ is Pisot, then x is "normal in base β", in the sense that the sequence $(x\beta^n)_{n\in\mathbb{N}}$ is uniformly distributed modulo one. We work with the notion of *P-martingale*, a generalization of martingales to non-uniform distributions, and show that a sequence over a finite alphabet is distributed according to an irreducible, invariant Markov measure P if an only if no P-martingale whose betting factors are computed by a deterministic finite automaton succeeds on it. This is a generalization of Schnorr and Stimm's characterization of normal sequences in integer bases. Our results use tools and techniques from symbolic dynamics, together with automata theory and algorithmic randomness.

1. Introduction

A weak notion of randomness for sequences over a finite alphabet $\Sigma = \{0, \dots, b-1\}$ ($b \in \mathbb{N}$) is *normality*, introduced by Borel in 1909. Normality may be regarded as a "law of large numbers" for blocks of events, in the sense that the average occurrences of a block $\sigma \in \Sigma^*$ of length n converge to $|\Sigma|^{-n}$. A real number x is called *normal in base b* ($b \in \mathbb{N}$) if its expansion in base b is normal. While almost all numbers are normal to all bases it is not too difficult to see that this notion is not base invariant. In fact for any multiplicatively independent bases b and b' the set of numbers normal to b but not normal to b' has full Hausdorff dimension [14]. We say a number x is *absolutely normal* if it is normal in all integer bases greater than one. It is not difficult to see that x is normal in base b if and only if the sequence $(xb^n)_{n\in\mathbb{N}}$ is u.d. modulo one, and then x is absolutely normal if and only if $(xb^n)_{n\in\mathbb{N}}$ is uniformly distributed (u.d.) modulo one for all integer $b > 1$.

Polynomial time randomness is another weak notion of randomness. We say that x is *polynomial time random in base b* if no martingale (a formalization of *betting strategy*) on the alphabet $\{0, \dots, b-1\}$ which is computable in polynomial time succeeds on the expansion of x in base b. A result of Schnorr [16] states that if x is polynomial time random in base b then x is normal in base b. It was recently shown [6] that polynomial time randomness is base invariant, so that being polynomial time random in a single base implies being normal for all bases, i.e. being absolutely normal. The converse is not true, since there are absolutely normal numbers which are computable in polynomial time [1,6,10], and these cannot be polynomial time random. The following question was left open in [6]:

* Corresponding author.
E-mail address: santiago@dc.uba.ar (S. Figueira).

http://dx.doi.org/10.1016/j.jcss.2015.04.005
0022-0000/

Question 1.1. Suppose that x is polynomial time random. Is the sequence $(x\beta^n)_{n\in\mathbb{N}}$ u.d. modulo one for all rational $\beta > 1$?

The distribution of $(x\beta^n)_{n\in\mathbb{N}}$ modulo one for rational β seems, however, fairly intractable. It is unknown, for instance, if $((3/2)^n)_{n\in\mathbb{N}}$ is u.d. modulo one. Our first main result is that there is a class of algebraic reals for which the question may be readily handled:

Theorem 1.2. *If x is polynomial time random then the sequence $(x\beta^n)_{n\in\mathbb{N}}$ is u.d. modulo one for all Pisot $\beta > 1$.*

Observe that any non-integer Pisot β is irrational, and as a consequence of a result of Brown, Moran and Pearce [4, Theorem 2], there are uncountably many reals which are absolutely normal but $(x\beta^n)_{n\in\mathbb{N}}$ is not u.d. modulo one.

The formulation of normality to integer bases β in terms of modulo one uniform distribution allows us to understand normality as equivalent to what ergodic theory calls *genericity*, an equivalence which boils down to two facts: 1) the map $T_\beta(x) = (\beta x) \bmod 1$ on $[0, 1)$ is equivalent to a "shift" rightwards in the space of sequences $\{0, \dots, \beta - 1\}^{\mathbb{N}}$ when x is mapped to its base β expansion; 2) $(x\beta^n) \bmod 1 = T_\beta^n(x)$.

When a non-integer base β is considered, 2) is immediately false, while 1) has no clear reformulation, since there is no obvious candidate for a space of sequences that "represent" numbers in base β. It is here that the theory of β-shifts and β-representations, developed, among others, by Parry [12] and Bertrand [2], helps fill in the missing pieces.

Once the space of sequences that represent numbers in the base β (using symbols from $\Sigma = \{0, \dots, \lceil\beta\rceil - 1\}$) is defined, it is equipped with a natural shift transformation and a measure P_β called the *Parry measure*, which plays the same role that the uniform or Lebesgue measure played in integer representation. Indeed, a result by Bertrand says that, when β is Pisot, if a real number x has a β-expansion that is distributed according to P_β (this is the analogue notion to being "normal in base β"), then $(x\beta^n)_{n\in\mathbb{N}}$ is u.d. modulo one.

To see how this is useful for the proof of Theorem 1.2, let us say we have a number z such that $(z\beta^n)_{n\in\mathbb{N}}$ is not u.d. modulo one. Then, by Bertrand's theorem, its β-representation would have some block σ whose average occurrences do not converge to $P_\beta(\sigma)$. We would then want to construct a polynomial time martingale that succeeds by betting on that block, as is done in the integer base case.

However, this cannot be done in a straightforward manner, since the martingale condition as used in the algorithmic randomness literature, assumes outcomes should be distributed according to the uniform measure.

We work with a generalized definition of martingales which captures the idea of a "fair" betting strategy when expansions are supposed to obey some non-uniform distribution P. Indeed, this definition of a *P-martingale* will capture the broader sense of *martingale* as it is used in probability theory. In this setting, not only may the probability of the next symbol be different from $|\Sigma|^{-1}$, it may also show all forms of conditional dependence on the preceding symbols. It should be noted that randomness notions under measures different from Lebesgue have already been considered in, for example, [15].

Schnorr and Stimm [17] show that a sequence is normal in base b if and only if no martingale on the alphabet of b digits whose betting factors are computed by a deterministic finite automaton (DFA) succeeds on the expansion of x in base b. Our second main result is a generalization of this last statement in terms of P-martingales:

Theorem 1.3. *A sequence is distributed according to an irreducible, invariant Markov measure P if an only if no P-martingale whose betting factors are computed by a DFA succeeds on it.*

The importance of Markov measures is that they exhibit enough memorylessness to make them compatible with the memoryless structure of a DFA.

As regards β-representations, a second result by Bertrand establishes that for β Pisot P_β, the natural measure on β-expansions, is "hidden" Markov. By extending Theorem 1.3 to hidden Markov measures we are able to construct a P_β-martingale generated by a DFA that succeeds on the β-expansion of z. We use the polynomial time computability of the β-expansion and of the measure P_β to show that an integer base (i.e. classical) martingale which succeeds on z can be constructed from our P_β-martingale, following the same ideas used in [6].

1.1. Outline

The paper is organized as follows. In Section 2 we introduce some basics from symbolic dynamics, mainly the definition of Markov and sofic subshifts, and the notion of sequences distributed according to invariant measures P over the shift. In Section 3 we introduce the notion of P-(super)martigales and show the characterization given by Theorem 1.3. In Section 4 we introduce some definitions and results regarded to representation of reals in non-integer bases, in particular, Pisot bases. Finally, in Section 5 we put all pieces together to get Theorem 1.2.

2. Subshifts and measures

Throughout this work Σ will denote an alphabet of finitely many symbols, which will be denoted by a, b, c, etc. The set of all words over the alphabet Σ will be denoted by Σ^*, and the set of all words of length k over the alphabet Σ